Solvable Irreducible Equations of Prime Degrees.

BY GEORGE PAXTON YOUNG, *Toronto, Canada.*

OBJECT OF THE PAPER.

§1. Let $F(x) = 0$ be an irreducible solvable equation of the m^{th} degree, m prime, with roots r_1, r_2, etc. The equation being understood to have been deprived of its second term, its roots are of the forms

$$\left.\begin{aligned} mr_1 &= \Delta_1^{\frac{1}{m}} + a_1\Delta_1^{\frac{2}{m}} + b_1\Delta_1^{\frac{3}{m}} + \ldots + c_1\Delta_1^{\frac{m-1}{m}} \\ mr_2 &= \omega\Delta_1^{\frac{1}{m}} + \omega^2 a_1\Delta_1^{\frac{2}{m}} + \omega^3 b_1\Delta_1^{\frac{3}{m}} + \ldots + \omega^{m-1}c_1\Delta_1^{\frac{m-1}{m}} \\ mr_3 &= \omega^2\Delta_1^{\frac{1}{m}} + \omega^4 a_1\Delta_1^{\frac{2}{m}} + \omega^6 b_1\Delta_1^{\frac{3}{m}} + \ldots + \omega^{2(m-1)}c_1\Delta_1^{\frac{m-1}{m}}, \end{aligned}\right\} \tag{1}$$

and so on; where ω is a primitive m^{th} root of unity; and a_1, b_1, etc., are rational functions of Δ_1. If we call

$$\Delta_1^{\frac{1}{m}},\ a_1\Delta_1^{\frac{2}{m}},\ b_1\Delta_1^{\frac{3}{m}},\ \ldots,\ c_1\Delta_1^{\frac{m-1}{m}}, \tag{2}$$

the separate members of mr_1, I propose first of all to establish the fundamental theorem, that *the separate members of the root r_1 can be arranged in groups G_1, G_2, etc., such that any symmetrical function of the terms in any one of the groups is a rational function of the root* (§8). The groups G_1, G_2, etc., may be defined more exactly as follows. The m^{th} powers of the terms in (2) are the roots of a rational equation of the $(m-1)^{\text{th}}$ degree auxiliary to $F(x) = 0$. Should the auxiliary not be irreducible, it can be broken, after the rejection of roots equal to zero, into rational irreducible sub-auxiliaries. This being so, the terms constituting any one of the groups G_1, G_2, etc., are those separate members of r_1, which, severally multiplied by m, are m^{th} roots of the roots of the auxiliary, provided the auxiliary be irreducible; but, when the auxiliary is not irreducible, the terms constituting any one of the groups G_1, G_2, etc., are m^{th} roots of the roots of a sub-auxiliary. *From the fundamental theorem above enunciated can be deduced as a corollary the theorem of Galois, that r_1 is a rational function of r_2 and r_3.* In fact,

any symmetrical function of those separate members of r_1 which constitute any one of the groups G_1, G_2, etc., is a rational function of r_2 and r_3 (§13). Not only is it proved that r_1 is a rational function of r_2 and r_3, but *the investigation shows how the function is formed.* An instance in verification is given (§15). It incidentally appears that if c be the number of terms in any one of the groups G_1, G_2, etc., *the sum of a cycle of c primitive m^{th} roots of unity is a rational function of r_1 and r_2* (§17).

PRELIMINARY STATEMENTS.

§2. Use will be made of certain general laws of the structure of the roots of equations, that were established in an article published in this Journal (Vol. VI), entitled "Principles of the Solution of Equations of the Higher Degrees." It was there shown that if

$$\Delta_1,\ \Delta_2,\ \ldots,\ \Delta_c, \tag{3}$$

be the unequal particular cognate forms (see "Principles," §9) of the generic expression Δ under which Δ_1 falls, there are m^{th} roots

$$\Delta_1^{\frac{1}{m}},\ \Delta_2^{\frac{1}{m}},\ \ldots,\ \Delta_c^{\frac{1}{m}}, \tag{4}$$

of the expressions in (3), such that the value of r_1 can be exhibited not only as in the first of equations (1), but also in the following ways:

$$\left.\begin{aligned} mr_1 &= \Delta_2^{\frac{1}{m}} + a_2\Delta_2^{\frac{2}{m}} + \ldots + c_2\Delta_2^{\frac{m-1}{m}} \\ mr_2 &= \Delta_3^{\frac{1}{m}} + a_3\Delta_3^{\frac{2}{m}} + \ldots + c_3\Delta_3^{\frac{m-1}{m}}, \end{aligned}\right\} \tag{5}$$

and so on; where a_2, b_2, etc. are what a_1, b_1, etc. become in passing from Δ_1 to Δ_2; and a_3, b_3, etc. what they become in passing to Δ_3; and so on. The separate members of mr_1, as it is expressed in the first line of (5), are

$$\Delta_2^{\frac{1}{m}},\ a_2\Delta_2^{\frac{2}{m}},\ \ldots,\ c_2\Delta_2^{\frac{m-1}{m}}, \tag{6}$$

§3. The sum of the terms in (6) is m times the same root of the equation $F(x)=0$ as the sum of those in (2). This implies, as was proved in the "Principles," that the terms in (6) are severally equal, in some order, to those in (2). Because Δ_2 and Δ_1 are unequal, $\Delta_2^{\frac{1}{m}}$ and $\Delta_1^{\frac{1}{m}}$ are unequal. Therefore they are equal to distinct members of mr_1 as these are expressed in (2). In like manner the terms in (4) are severally equal to distinct separate members of mr_1.

§4. It can be shown that a cycle of c primitive roots of unity

$$\omega,\ \omega^{\lambda},\ \omega^{\lambda^2},\ \ldots,\ \omega^{\lambda^{c-1}}, \tag{7}$$

can be formed; and that the terms in (2) to which those in (4) are equal are those in which the indices of the powers of $\Delta_1^{\frac{1}{m}}$ are the numbers

$$1, \lambda, \lambda^2, \ldots, \lambda^{c-1}, \tag{8}$$

with multiples of m rejected. When (7) is called a cycle, the meaning is that no term in the series after the first is equal to the first, but $\omega^{\lambda^c} = \omega$. For brevity's sake I may be allowed, where there is no danger of mistake, if $g_1 \Delta_1^{\frac{n}{m}}$ be a term in (2), to speak of it as $g_1 \Delta_1^{\frac{\lambda^a}{m}}$, n being λ^a with multiples of m left out. In like manner if

$$\omega, \omega^b, \omega^{b^2}, \ldots, \omega^{b^{z-1}}, \tag{9}$$

be a cycle of primitive m^{th} roots of unity, and if there be a term in (2) in which the index of the power of $\Delta_1^{\frac{1}{m}}$ is b^a, the term may be spoken of as $\sigma_1 \Delta_1^{\frac{b^a}{m}}$, where multiples of m must be understood to be rejected from b^a. Let then $\Delta_1^{\frac{1}{m}}$ and $\alpha_1 \Delta_1^{\frac{b}{m}}$ in (2) be equal to distinct terms in (4). I will first show that there are terms in (2) in which the indices of the powers of $\Delta_1^{\frac{1}{m}}$ are the indices of the powers of ω in (9). Let $\Delta_2^{\frac{1}{m}}$ be the term in (4) to which $\alpha_1 \Delta_1^{\frac{b}{m}}$ is by hypothesis equal. The term in (6) to which $\alpha_1 \Delta_1^{\frac{b}{m}}$ in (2) corresponds is $\alpha_2 \Delta_2^{\frac{b}{m}}$. Because $\Delta_2^{\frac{1}{m}} = \alpha_1 \Delta_1^{\frac{b}{m}}$, $\alpha_2 \Delta_2^{\frac{b}{m}} = \alpha_2 \alpha_1^b \Delta_1^{\frac{b^2}{m}}$. Hence the term in (2) to which $\alpha_2 \Delta_2^{\frac{b}{m}}$ in (6) is equal must be $\beta_1 \Delta_1^{\frac{b^2}{m}}$; for, if it were any other term than that mentioned, say $\tau_1 \Delta_1^{\frac{n}{m}}$ we should have

$$\tau_1 \Delta_1^{\frac{n}{m}} = \alpha_2 \alpha_1^b \Delta_1^{\frac{b^2}{m}}, \tag{10}$$

where b^2 with multiples of m left out, is not equal to n. But, from the state in which algebraical expressions are supposed in the "Principles" to be presented, since no surds occur in τ_1, α_1 or α_2 except such as are found in Δ_1 or Δ_2, the equation (10) would require τ_1 and $\alpha_2 \alpha_1^b$ to be separately zero; and this again would make $\alpha_2 \Delta_2^{\frac{b}{m}}$, and therefore $\alpha_1 \Delta_1^{\frac{b}{m}}$, and therefore $\Delta_2^{\frac{1}{m}}$, and therefore $\Delta_1^{\frac{1}{m}}$, zero; which is impossible. Therefore $\alpha_2 \Delta_2^{\frac{b}{m}} = \beta_1 \Delta_1^{\frac{b^2}{m}}$. But, because $\alpha_1 \Delta_1^{\frac{b}{m}} = \Delta_2^{\frac{1}{m}}$, $\alpha_1 \Delta_1^{\frac{b}{m}}$ is one of the particular cognate forms of $\Delta^{\frac{1}{m}}$. Therefore also $\alpha_2 \Delta_2^{\frac{b}{m}}$ is a particular cognate form of $\Delta^{\frac{1}{m}}$, which may be taken to be $\Delta_3^{\frac{1}{m}}$. Therefore $\beta_1 \Delta_1^{\frac{b^2}{m}}$ is equal to $\Delta_3^{\frac{1}{m}}$, a term in (4). In like manner it follows that all the terms in (2) in which the indices of the powers of $\Delta_1^{\frac{1}{m}}$ are any of the indices of the powers of ω in (9) are equal to terms in (4). Let

$$\Delta_1^{\frac{1}{m}}, \alpha_1 \Delta_1^{\frac{b}{m}}, \beta_1 \Delta^{\frac{b^2}{m}}, \ldots, \gamma_1 \Delta_1^{\frac{b^{z-1}}{m}}, \tag{11}$$

be terms in (2) severally equal to the terms in (4),

$$\Delta_1^{\frac{1}{m}},\ \Delta_2^{\frac{1}{m}},\ \Delta_3^{\frac{1}{m}},\ \ldots,\ \Delta_z^{\frac{1}{m}}. \tag{12}$$

We may assume $\alpha_1 \Delta_1^{\frac{b}{m}}$ to have been so chosen that there is no term in (2), as $\sigma_1 \Delta_1^{\frac{h}{m}}$, equal to a term in (4), and such that when the cycle

$$\omega,\ \omega^h,\ \omega^{h^2},\ \ldots,\ \omega^{h^{v-1}}, \tag{13}$$

is formed, v is greater than z. In that case, z must be equal to c. For suppose if possible that z is less than c. Then there is a term in (4) distinct from those in (12), say $\Delta_{z+1}^{\frac{1}{m}}$, equal to a term in (2) in which the index of the power of $\Delta_1^{\frac{1}{m}}$ is not a power of b, which term in (2) may be taken to be $g_1 \Delta_1^{\frac{bd}{m}}$, d not being a power of b. Then, just as we proved that, because $\Delta_1^{\frac{1}{m}}$ and $\alpha_1 \Delta_1^{\frac{b}{m}}$ are terms in (2) equal to terms in (4), any term in (2) having for the index of the power of $\Delta_1^{\frac{1}{m}}$ any of the indices of the powers of ω in (9) must be equal to a term in (4), we can show that because $\Delta_1^{\frac{1}{m}}$ and $\Delta_1^{\frac{bd}{m}}$ are terms in (2) equal to terms in (4), there must be a term in (4) equal to one in (2) in which the index of the power of $\Delta_1^{\frac{1}{m}}$ is $b^W d^W$, W being any whole number. Hence there is a distinct term in (4) equal to a term in (2) corresponding to each distinct term in the cycle

$$\omega,\ \omega^{bd},\ \omega^{b^2d^2},\ \text{etc.}$$

Putting h for bd, this cycle is identical with (13). And since d is not a power of b, the number of terms in the cycle ω, ω^{bd}, etc. is greater than that in (9). Hence the number of terms in (13) exceeds that in (9). That is, v is greater than z; which, by hypothesis, is impossible. Hence z cannot be less than c. And it is not greater, because all the terms in (12) are contained in (4). Therefore $z = c$. Therefore there is a cycle of c primitive m^{th} roots of unity, which may be taken to be (7); and, comparing this with (9), λ may be taken to be b; and the series (11), which may now be written

$$\Delta_1^{\frac{1}{m}},\ \alpha_1 \Delta_1^{\frac{\lambda}{m}},\ \beta_1 \Delta_1^{\frac{\lambda^2}{m}},\ \ldots,\ \gamma_1 \Delta_1^{\frac{\lambda^{c-1}}{m}}, \tag{14}$$

has the same number of terms as (4). Consequently the terms in (14) are those terms in (2) which are severally equal to terms in (4).

§5. Take E_1 a rational function of Δ_1; let the generic expression (§2) of which it is a particular form be E; and when Δ_1 passes successively into the c terms in (4), let E_1 become successively

$$E_1,\ E_2,\ \ldots,\ E_c. \tag{15}$$

By the "Principles," Prop. III, each of the unequal particular cognate forms of Δ occurs the same number of times in the series of the cognate forms. Therefore the entire series of the particular cognate forms is made up of k groups of c terms each, the terms in any one of the groups being equal to those in each of the others. These k groups may be written

$$\left.\begin{array}{llll} \Delta_1, & \Delta_2, & \ldots, & \Delta_c, \\ \Delta_{c+1}, & \Delta_{c+2}, & \ldots, & \Delta_{2c}, \\ \Delta_{2c+1}, & \Delta_{2c+2}, & \ldots, & \Delta_{3c}, \end{array}\right\} \tag{16}$$

and so on. The entire series of the particular cognate forms of E must consist of k corresponding groups of c terms each,

$$\left.\begin{array}{llll} E_1, & E_2, & \ldots, & E_c, \\ E_{c+1}, & E_{c+2}, & \ldots, & E_{2c}, \\ E_{2c+1}, & E_{2c+2}, & \ldots, & E_{3c}, \end{array}\right\} \tag{17}$$

and so on; E_a being what E_1 becomes when Δ_1 becomes Δ_a.

§6. It is plain that if $\Delta_a = \Delta_z$, $E_a = E_z$. For, since Δ_a is a root of an equation of the c^{th} degree, any rational function of Δ_a may be expressed without using powers of Δ_a above the $(c-1)^{\text{th}}$. And E_a is a rational function of Δ_a. Therefore we may put

$$E_a = s + s_1\Delta_a + s_2\Delta_a^2 + \ldots + s_{c-1}\Delta_a^{c-1}$$

$$\text{and}\quad E_z = s + s_1\Delta_z + s_2\Delta_z^2 + \ldots + s_{c-1}\Delta_z^{c-1},$$

where s, s_1, etc. are rational. But, by hypothesis, $\Delta_a = \Delta_z$. Therefore $E_a = E_z$.

§7. This leads to the conclusion that any symmetrical function of the terms in (15) is rational. For, by §5, the terms in any line of (16) under the first are severally equal to those in the first line. Therefore, by §6, the terms in any line of (17) under the first are severally equal to those in the first. Let the unequal terms in the first line of (17) be $E_1, E_2, \ldots, E_n$. Let E_1 and E_2 occur α and β times respectively in the first line of (17); then they occur αk and βk times respectively in the k groups of (17). But, by the "Principles," Prop. III, each of the unequal particular cognate forms of E occurs the same number of times in the entire series. Therefore αk and βk are equal, and $\alpha = \beta$. That is to say, E_1 and E_2 occur the same number of times in the first line of (17). In like manner all the unequal terms in the first line of (17) occur the same number of times in that line. Therefore, if $X_1 = 0$ be the equation whose roots are E_1, $E_2, \ldots, E_n$, and $X = 0$ be the equation whose roots are $E_1, E_2, \ldots, E_c$, $X = X_1^{\alpha}$. But, by the "Principles," Prop. III, X_1 is rational. Therefore X is

rational. This implies that any symmetrical function of the roots of the equation $X = 0$, that is, of the terms in (14), is rational.

Symmetrical Functions of the terms in (4).

§8. I will now establish the fundamental theorem that *any symmetrical function of those separate members of mr_1, which are m^{th} roots of the roots of the equation auxiliary or of an equation sub-auxiliary to the equation $F(x) = 0$ is a rational function of r_1.* When $c = m - 1$, the terms in (3) are the roots of the irreducible auxiliary (see §1) to $F(x) = 0$. When c is less than $m - 1$, they are the roots of a sub-auxiliary. What we need then to make out is, that *any symmetrical function of the terms in* (4) *is a rational function of r_1.*

§9. From the first of equations (1), $\Delta_1^{\frac{1}{m}}$ is a root of the equation

$$c_1 x^{m-1} + \ldots + a_1 x^2 + x - mr_1 = 0, \tag{18}$$

being at the same time a root of the equation

$$x^m - \Delta_1 = 0. \tag{19}$$

Now $\omega\Delta_1^{\frac{1}{m}}$ is not a root of (18); for, if it were, we should have

$$c_1 (\omega\Delta_1^{\frac{1}{m}})^{m-1} + \ldots + (\omega\Delta_1^{\frac{1}{m}}) - mr_1 = 0;$$

and therefore, by comparison with the second of equations (1), $r_2 = r_1$, which is impossible. In the same way no root of (19) except $\Delta_1^{\frac{1}{m}}$ is a root of (18). Therefore the highest common measure of the expressions on the left of (18) and (19) is $x - Q$, where Q is a rational function of r_1, Δ_1, a_1, etc., and therefore, by §1, a rational function of r_1 and Δ_1. We may express this, since $\Delta_1^{\frac{1}{m}}$ is the value of Q, by putting

$$\left.\begin{aligned} \Delta_1^{\frac{1}{m}} &= f(r_1, \Delta_1). \\ \text{Similarly, from (5),}\quad \Delta_2^{\frac{1}{m}} &= f(r_1, \Delta_2), \\ \Delta_3^{\frac{1}{m}} &= f(r_1, \Delta_3), \end{aligned}\right\} \tag{20}$$

and so on. Since f here denotes a rational function, if the sum of the c expressions $\Delta_1^{\frac{1}{m}}$, $\Delta_2^{\frac{1}{m}}$, etc., be $\frac{N}{D}$, both N and D must, from (20), be composed of terms of the type $E' r_1^2$; where E' is a symmetrical function of the c expressions, Δ_1, Δ_2, etc., and is therefore, by §7, rational. Consequently the sum of the c terms $\Delta_1^{\frac{1}{m}}$, $\Delta_2^{\frac{1}{m}}$, etc. is a rational function of r_1. In the same way any symmetrical function of these terms is a rational function of r_1. Thus the fundamental theorem is established.

§10. Setting out from $\Delta_1^{\frac{1}{m}}$, one of the separate members of mr_1, and taking the c unequal particular cognate forms of the generic expression Δ under which Δ_1 falls, we have found that certain m^{th} roots of these, being separate members of mr_1, satisfy equations (20), and therefore that any symmetrical function of these m^{th} roots is a rational function of r_1. If now we set out from an m^{th} root of Δ_1 distinct from $\Delta_1^{\frac{1}{m}}$, say $\omega\Delta_1^{\frac{1}{m}}$, one of the separate members of mr_2, we can in the same way demonstrate that there is another group of m^{th} roots of the terms in (3), say

$$\omega\Delta_1^{\frac{1}{m}}, \text{ or } D_1^{\frac{1}{m}}, \; D_2^{\frac{1}{m}}, \; D_3^{\frac{1}{m}}, \; \ldots, \; D_c^{\frac{1}{m}}, \tag{21}$$

by means of which equations corresponding to (20) can be formed.

§11. It is readily seen that the series (21) is identical with

$$\omega\Delta_1^{\frac{1}{m}}, \; \omega^{\lambda}\Delta_2^{\frac{1}{m}}, \; \omega^{\lambda^2}\Delta_3^{\frac{1}{m}}, \; \ldots, \; \omega^{\lambda^{c-1}}\Delta_c^{\frac{1}{m}}. \tag{22}$$

For, by §4, the series (4) is identical with (14), which may again be written down:

$$\Delta_1^{\frac{1}{m}}, \; \alpha_1\Delta_1^{\frac{\lambda}{m}}, \; \beta_1\Delta_1^{\frac{\lambda^2}{m}}, \; \ldots, \; \gamma_1\Delta_1^{\frac{\lambda^{c-1}}{m}}. \tag{23}$$

Taking the term $\Delta_2^{\frac{1}{m}}$ in (4), we saw that $\Delta_2^{\frac{1}{m}} = \alpha_1\Delta_1^{\frac{\lambda}{m}}$. Therefore $\alpha_1(\omega\Delta_1^{\frac{1}{m}})^{\lambda} = \omega^{\lambda}\Delta_2^{\frac{1}{m}}$. But, $\alpha_1\Delta_1^{\frac{\lambda}{m}}$ being one of the separate members of mr_1 in (1), $\alpha_1(\omega\Delta_1^{\frac{1}{m}})^{\lambda}$ is the corresponding separate member of mr_2. Therefore $\omega^{\lambda}\Delta_2^{\frac{1}{m}}$ is equal to one of the members of mr_2 in (1). And its m^{th} power is Δ_2, one of the particular cognate forms of Δ. Therefore it must be a term in (21), because (21) is made up of those separate members of mr_2 whose m^{th} powers are particular cognate forms of Δ. We may take $D_2^{\frac{1}{m}}$ to be equal to $\omega^{\lambda}\Delta_2^{\frac{1}{m}}$. In the same way $D_3^{\frac{1}{m}} = \omega^{\lambda^2}\Delta_3^{\frac{1}{m}}$, and so on.

§12. Hence the equations corresponding to (20), which can be formed by means of the terms in (21), are

$$\left.\begin{aligned} \omega\Delta_1^{\frac{1}{m}} &= f(r_2, \Delta_1) \\ \omega^{\lambda}\Delta_2^{\frac{1}{m}} &= f(r_2, \Delta_2) \\ \omega^{\lambda^2}\Delta_3^{\frac{1}{m}} &= f(r_2, \Delta_3), \end{aligned}\right\} \tag{24}$$

and so on. In the functions on the right of (24), Δ_1, Δ_2, etc. remain as in (20), because the passage from Δ_1 to D_1 or $(\omega\Delta_1^{\frac{1}{m}})^m$, and so on, makes no change in Δ_1, Δ_2, etc. In like manner,

$$\left.\begin{aligned} \omega^2\Delta_1^{\frac{1}{m}} &= f(r_3, \Delta_1) \\ \omega^{2\lambda}\Delta_2^{\frac{1}{m}} &= f(r_3, \Delta_2) \\ \omega^{2\lambda^2}\Delta_3^{\frac{1}{m}} &= f(r_3, \Delta_3), \end{aligned}\right\} \tag{25}$$

and so on.

GALOIS' THEOREM.

§13. We can now deduce Galois' Theorem, that *r_1 is a rational function of r_2 and r_3.* In fact, the separate members of r_1 can be arranged in groups such that any symmetrical function of the members in each group is a rational function of r_2 and r_3. One of the groups is obtained by dividing the terms in (4) severally by m. What we have to prove therefore is that *any symmetrical function of the terms in* (4) is a rational function of r_2 and r_3.

§14. Square both sides of (24), and divide by $\omega^2\Delta_1^{\frac{1}{m}}$ in the case of the first line, by $\omega^{2\lambda}\Delta_2^{\frac{1}{m}}$ in the case of the second, and so on. Then, keeping (25) in view,

$$\left.\begin{aligned} \Delta_1^{\frac{1}{m}} &= \frac{\{f(r_2,\Delta_1)\}^2}{\omega^2\Delta_1^{\frac{1}{m}}} = \frac{\{f(r_2,\Delta_1)\}^2}{f(r_3,\Delta_1)} \\ \Delta_2^{\frac{1}{m}} &= \frac{\{f(r_2,\Delta_2)\}^2}{\omega^{2\lambda}\Delta_2^{\frac{1}{m}}} = \frac{\{f(r_2,\Delta_2)\}^2}{f(r_3,\Delta_2)}, \end{aligned}\right] \tag{26}$$

and so on. By §7, the sum of the c expressions on the extreme right of (26), only two of which are written down, is a rational function of r_2 and r_3. Calling this $\phi(r_2, r_3)$,

$$\Delta_1^{\frac{1}{m}} + \Delta_2^{\frac{1}{m}} + \ldots + \Delta_c^{\frac{1}{m}} = \phi(r_2, r_3). \tag{27}$$

Thus the sum of the c separate members of mr_1 forming the group (4) is a rational function of r_2 and r_3. If $c = m - 1$, this is Galois' theorem. If c be less than $m - 1$, it may be shown as above that the sum of another quite distinct group of separate members of mr_1 is a rational function of r_2 and r_3. And so on till the series (2) is exhausted, so that Galois' theorem still holds. It is obvious that, in the same way in which (27) was obtained, any symmetrical function of the c expressions, $\Delta_1^{\frac{1}{m}}$, $\Delta_2^{\frac{1}{m}}$, etc. can be shown to be a rational function of r_2 and r_3.

LAW OF THE FORMATION OF THE FUNCTION; VERIFYING INSTANCE.

§15. It will be observed that, in the preceding section, *the law of the formation of the function $\phi(r_2, r_3)$ comes to light.* The rule is this: Take $x - Q$, the highest common measure of the expressions on the left of (18) and (19). The expression Q is $f(r_1, \Delta_1)$. Then

$$\phi(r_2, r_3) = \Sigma\left[\frac{\{f(r_2,\Delta_1)\}^2}{f(r_3,\Delta_1)}\right], \tag{28}$$

the expression on the right of (28) being the sum of the c expressions on the extreme right of (26).

§16. A simple verification is afforded by the equation

$$x^3 - \frac{x}{3} - \frac{4}{27} = 0.$$

Putting $\Delta_1 = 2 + \sqrt{3}$ and $\Delta_2 = 2 - \sqrt{3}$, the roots of the equation are

$$\begin{aligned} 3r_1 &= \Delta_1^{\frac{1}{3}} + \Delta_2 \Delta_1^{\frac{2}{3}} \\ 3r_2 &= \omega \Delta_1^{\frac{1}{3}} + \omega^2 \Delta_2 \Delta_1^{\frac{2}{3}} \\ 3r_3 &= \omega^2 \Delta_1^{\frac{1}{3}} + \omega \Delta_2 \Delta_1^{\frac{2}{3}}, \end{aligned}$$

ω being a primitive third root of unity. This gives $\dfrac{3r_1 + \Delta_2}{3r_1\Delta_2 + 1}$ as the value of Q. Then (28) becomes,

$$3r_1 = \phi(r_2, r_3) = \frac{\Delta_1 (3r_2 + \Delta_2)^2 (3r_3 + \Delta_1)}{(3r_2 + \Delta_1)^2 (3r_3 + \Delta_2)} + \frac{\Delta_2 (3r_2 + \Delta_1)^2 (3r_2 + \Delta_2)}{(3r_2 + \Delta_2)^2 (3r_3 + \Delta_1)}. \quad (29)$$

This result will perhaps most easily be seen to be accurate, if, by means of equations (30) immediately to be established, (29) be changed into

$$3r_1 = \frac{\omega^2 \Delta_1 (3r_2 + \Delta_2)}{3r_2 + \Delta_1} + \frac{\omega \Delta_2 (3r_2 + \Delta_1)}{3r_2 + \Delta_2}.$$

CYCLE OF c PRIMITIVE ROOTS OF UNITY.

§17. A result incidentally presenting itself is, that *the sum of a cycle of c primitive m^{th} roots of unity is a rational function of two of the roots of the equation* $F(x) = 0$. For, from (24), (25) and (20)

$$\left.\begin{aligned} \omega &= \frac{f(r_2, \Delta_1)}{f(r_1, \Delta_1)} = \frac{f(r_3, \Delta_1)}{f(r_2, \Delta_1)} = \dots \\ \omega^\lambda &= \frac{f(r_2, \Delta_2)}{f(r_1, \Delta_2)} = \frac{f(r_3, \Delta_2)}{f(r_2, \Delta_2)} = \dots \\ &\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \omega^{\lambda^{c-1}} &= \frac{f(r_2, \Delta_c)}{f(r_1, \Delta_c)} = \frac{f(r_3, \Delta_c)}{f(r_2, \Delta_c)} = \dots \end{aligned}\right\} \quad (30)$$

$$\therefore\ \omega + \omega^\lambda + \dots + \omega^{\lambda^{c-1}} = \Sigma \left\{ \frac{f(r_2, \Delta_1)}{f(r_1, \Delta_1)} \right\} = \Sigma \left\{ \frac{f(r_3, \Delta_1)}{f(r_2, \Delta_1)} \right\} = \dots$$

By §7, the sum of the m^{th} roots of unity in the cycle, ω, ω^λ, etc., as the sum is here obtained, is a rational function of r_2 and r_3, of r_3 and r_4, and so on.